FIG. 1

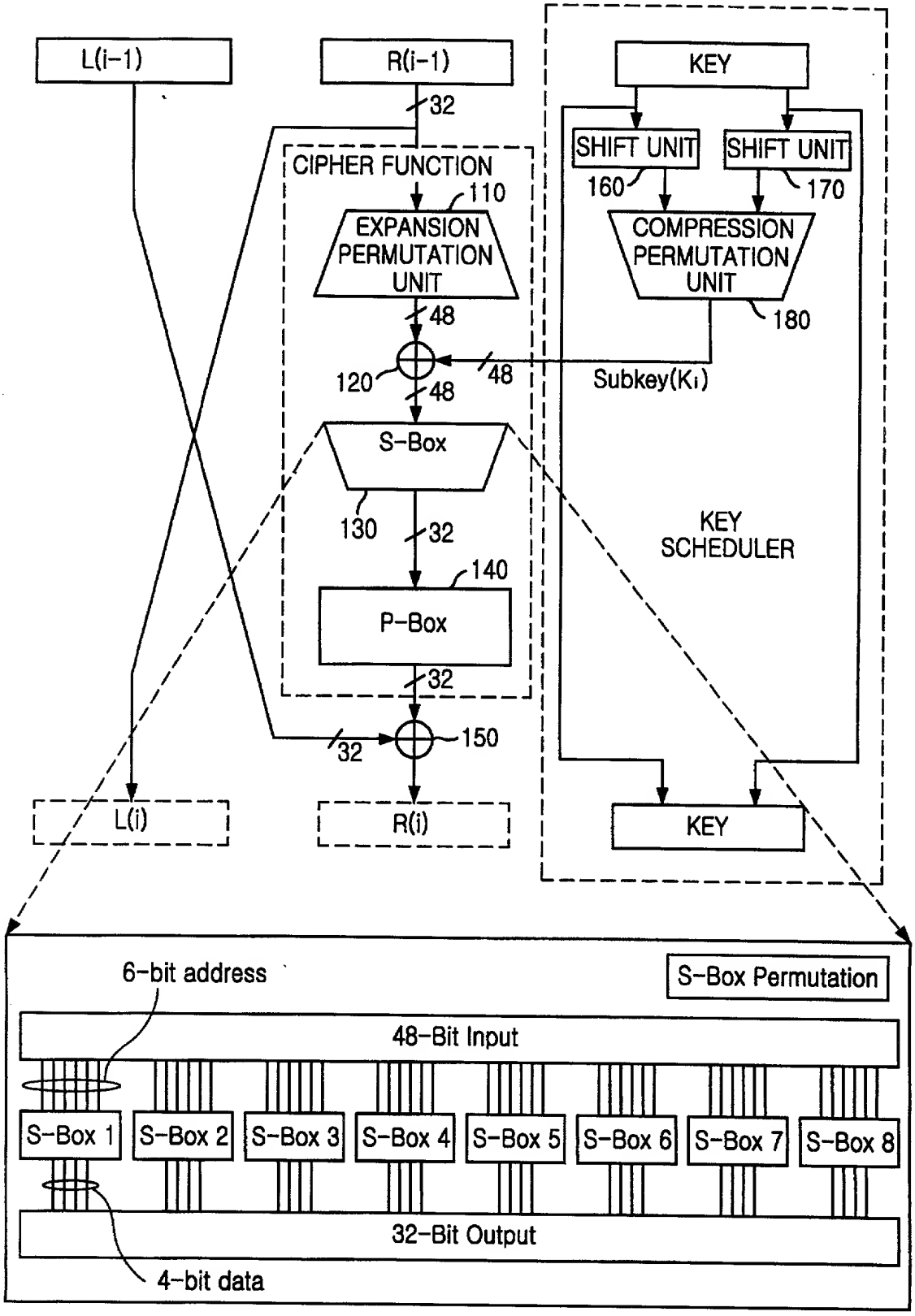
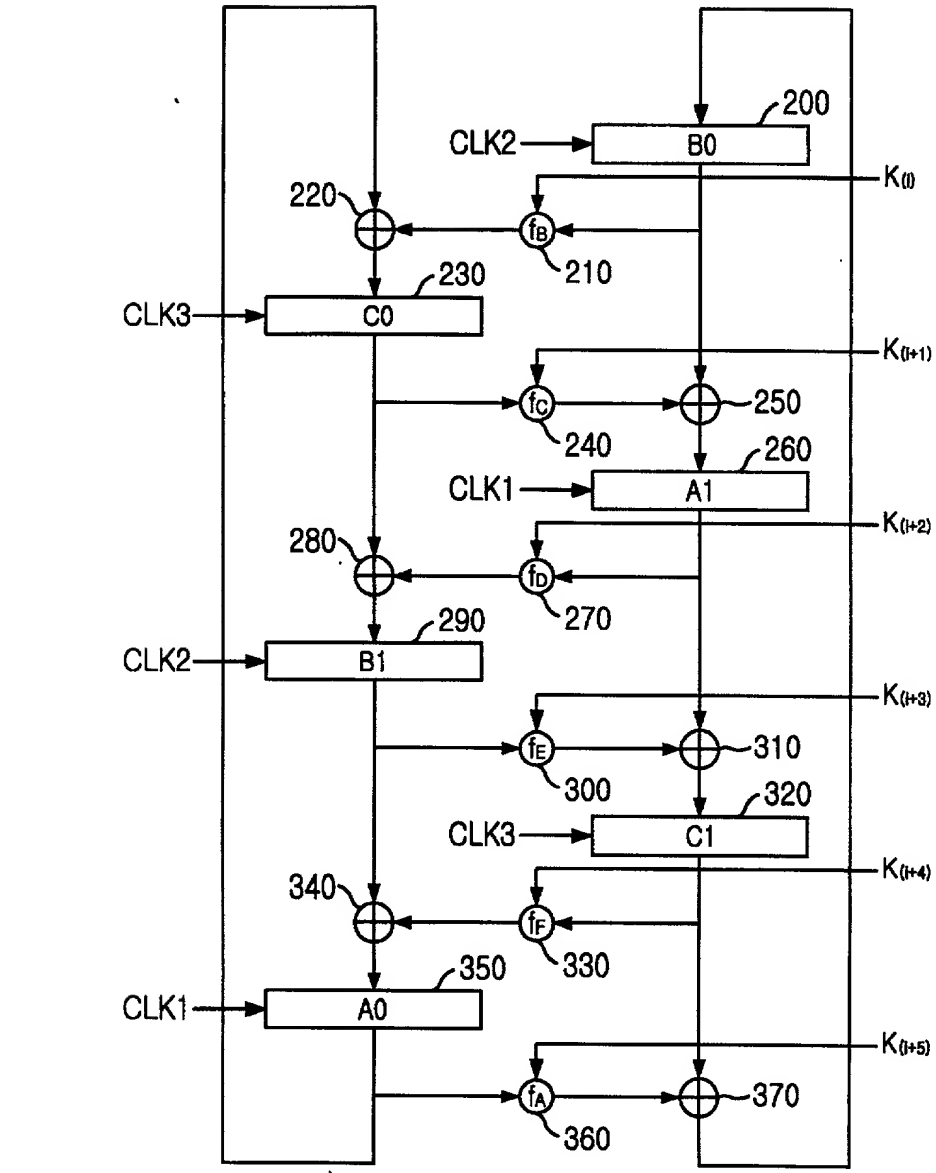

L(i-1)
R(i-1)
32
KEY
SHIFT UNIT
SHIFT UNIT
160
170
CIPHER FUNCTION
110
EXPANSION PERMUTATION UNIT
COMPRESSION PERMUTATION UNIT
180
48
120
48
48
Subkey(Ki)
S-Box
130
32
KEY SCHEDULER
140
P-Box
32
32
150
L(i)
R(i)
KEY
6-bit address
S-Box Permutation
48-Bit Input
S-Box 1
S-Box 2
S-Box 3
S-Box 4
S-Box 5
S-Box 6
S-Box 7
S-Box 8
32-Bit Output
4-bit data

FIG. 2


200
CLK2
B0
K(i)
220
fB
210
230
CLK3
C0
K(i+1)
fC
250
240
260
CLK1
A1
K(i+2)
280
fD
270
290
CLK2
B1
K(i+3)
fE
310
300
320
CLK3
C1
K(i+4)
340
fF
330
350
CLK1
A0
K(i+5)
fA
370
360

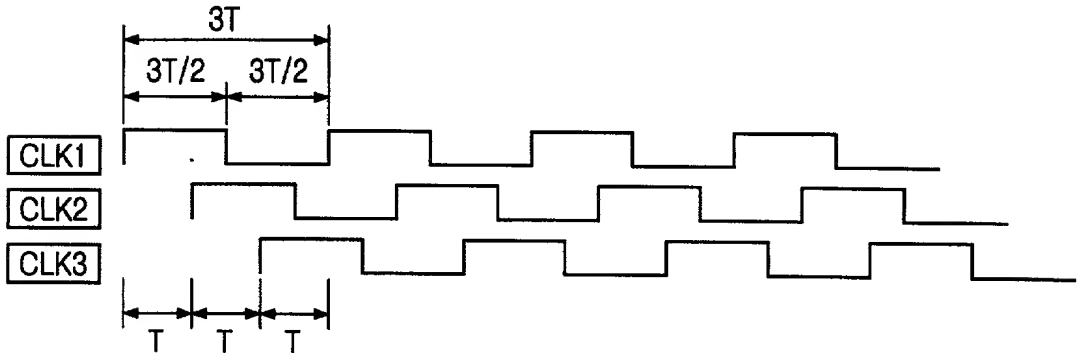

3T
3T/2
3T/2
CLK1
CLK2
CLK3
T
T
T

FIG. 3

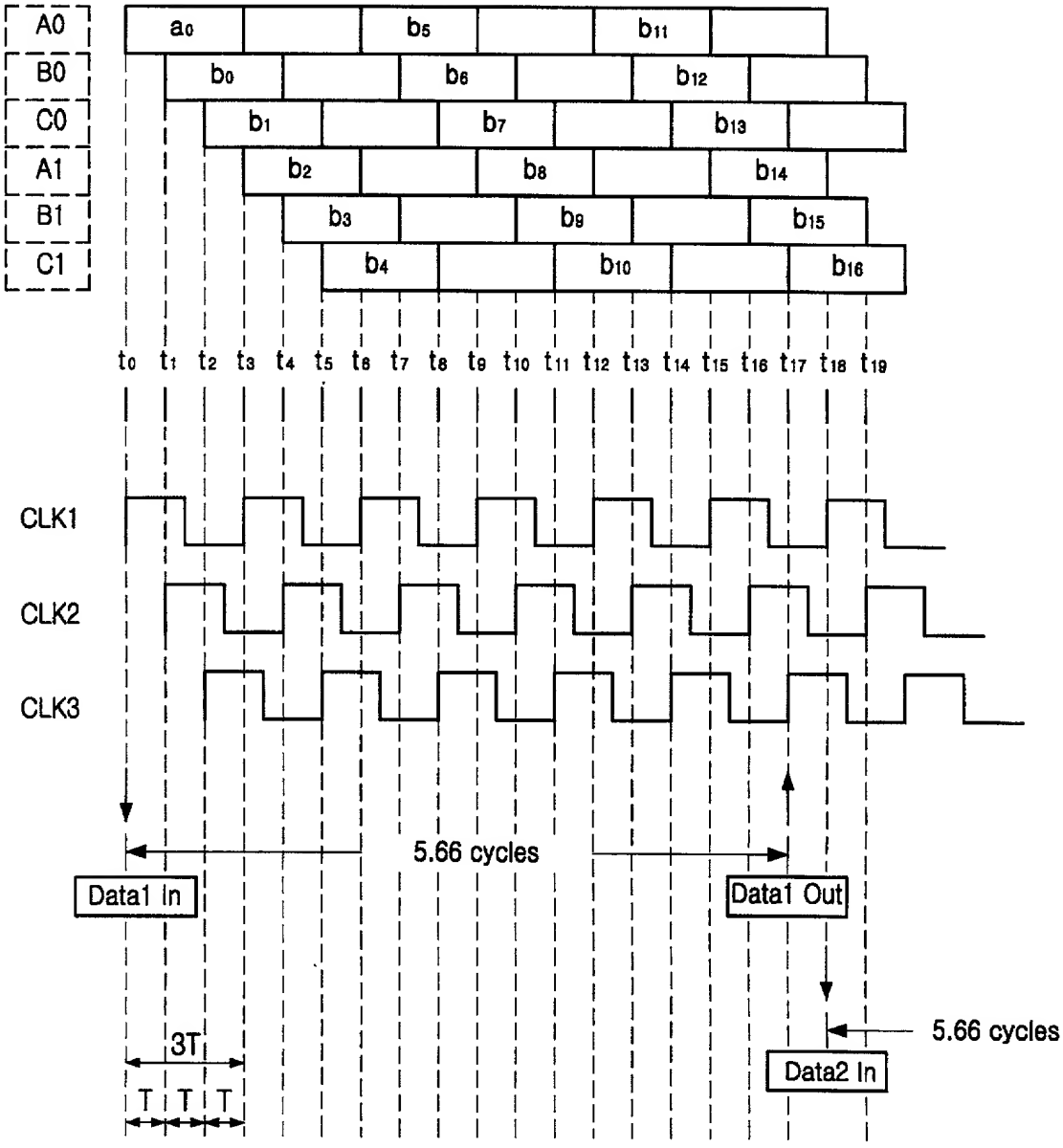

A0
B0
C0
A1
B1
C1
a0
b5
b11
b0
b6
b12
b1
b7
b13
b2
b8
b14
b3
b9
b15
b4
b10
b16
t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19
CLK1
CLK2
CLK3
5.66 cycles
Data1 In
Data1 Out
5.66 cycles
Data2 In
3T
T T T

FIG. 4

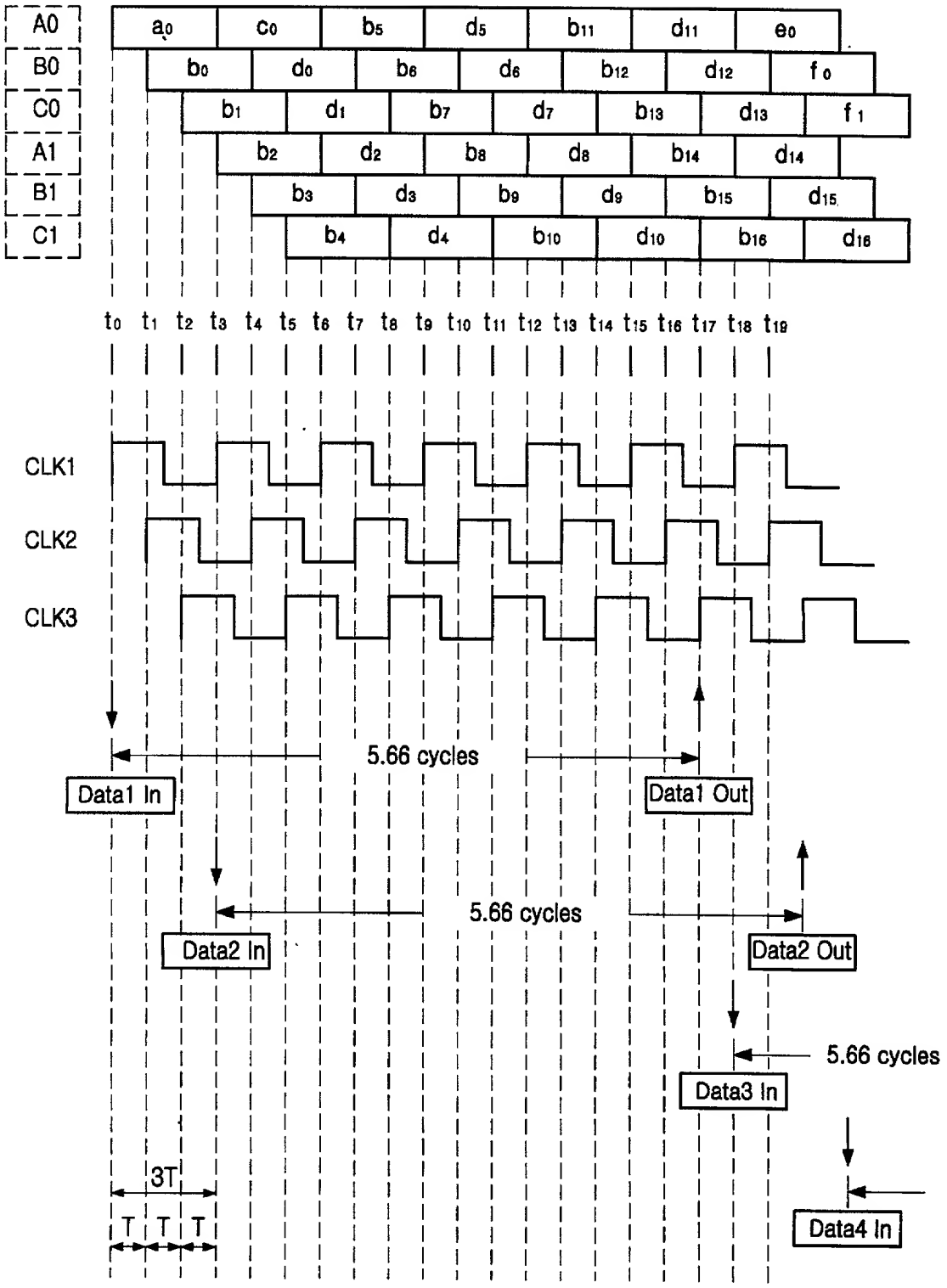

A0
B0
C0
A1
B1
C1
a0 c0 b5 d5 b11 d11 e0
b0 d0 b6 d6 b12 d12 f0
b1 d1 b7 d7 b13 d13 f1
b2 d2 b8 d8 b14 d14
b3 d3 b9 d9 b15 d15
b4 d4 b10 d10 b16 d16
t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19
CLK1
CLK2
CLK3
5.66 cycles
Data1 In
Data1 Out
5.66 cycles
Data2 In
Data2 Out
5.66 cycles
Data3 In
Data4 In
3T
T T T

FIG. 5

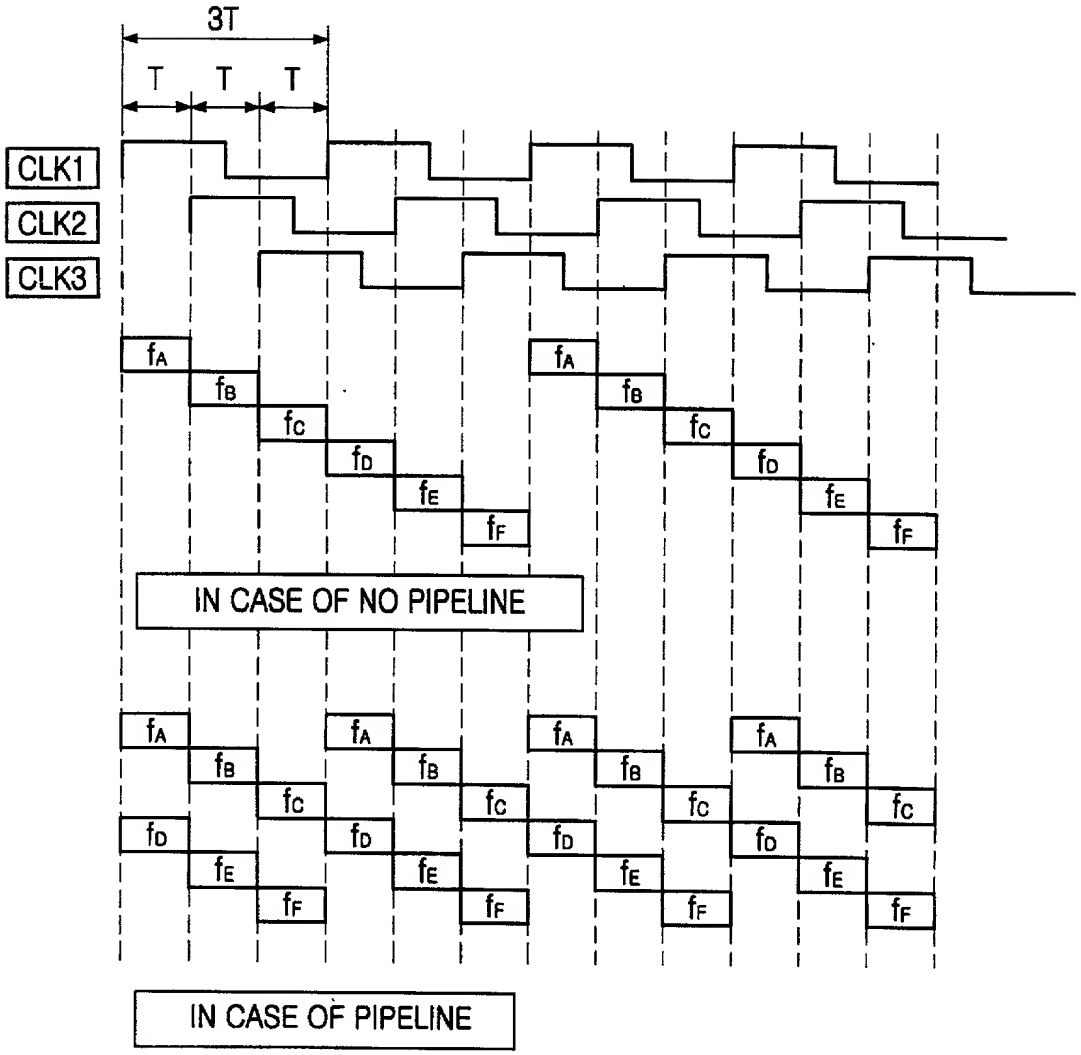

3T
T
T
T
CLK1
CLK2
CLK3
fA
fB
fC
fD
fE
fF
IN CASE OF NO PIPELINE
IN CASE OF PIPELINE

FIG. 6

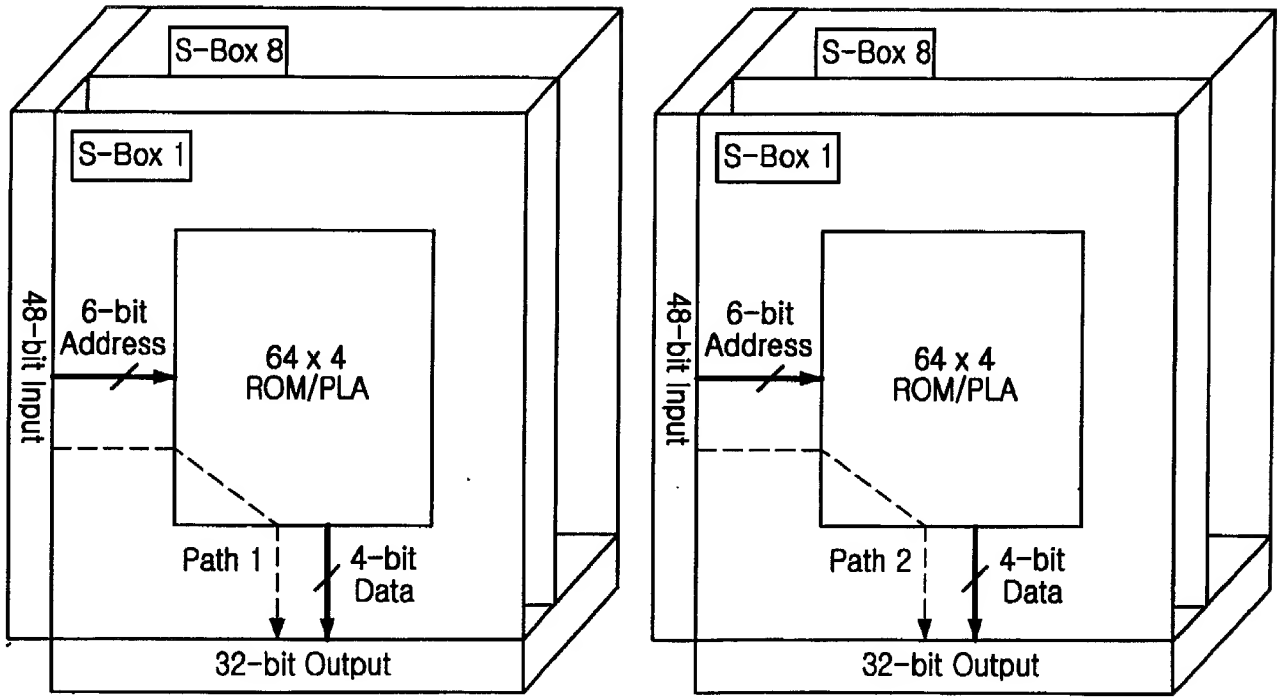


FIG. 7

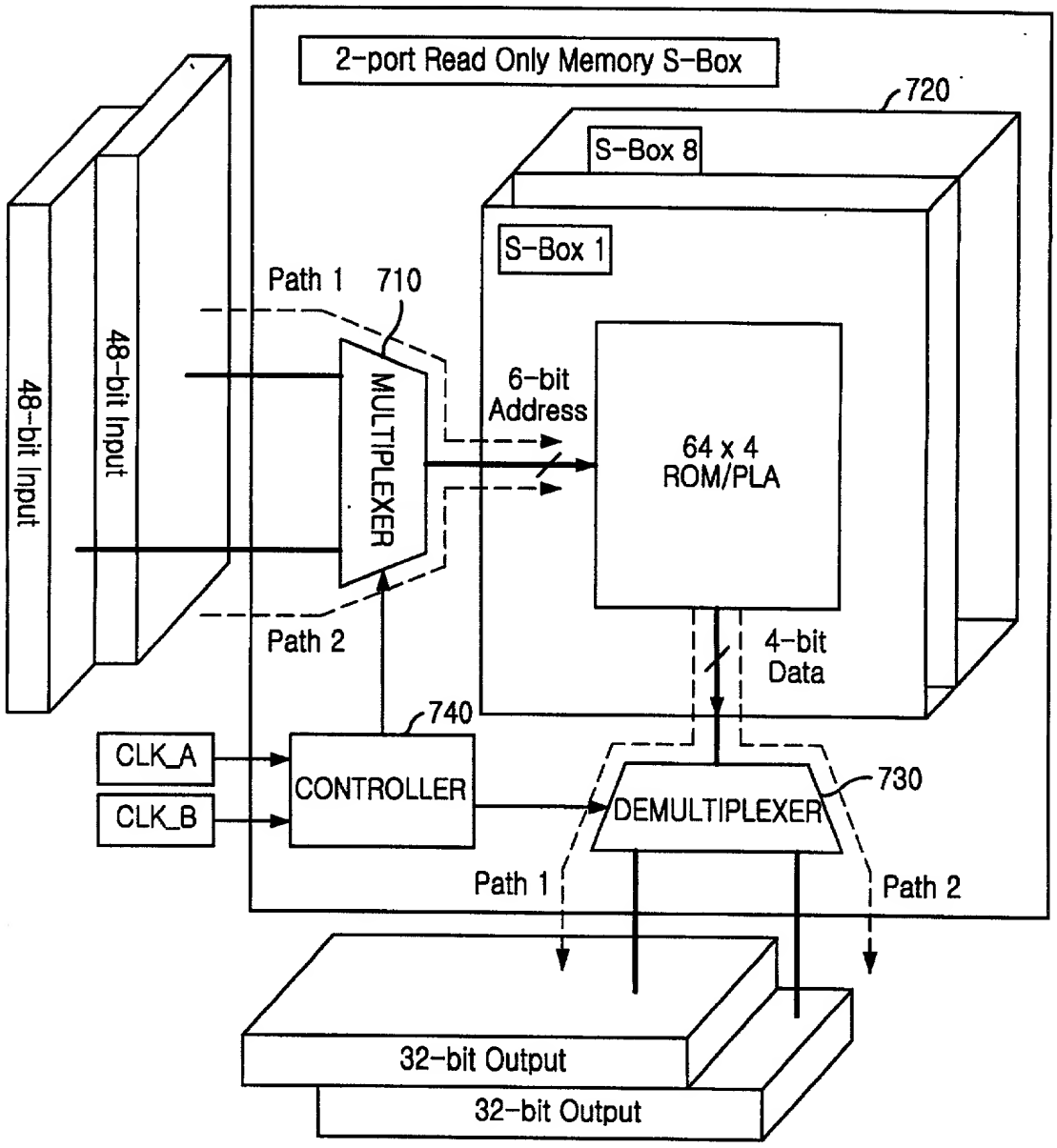
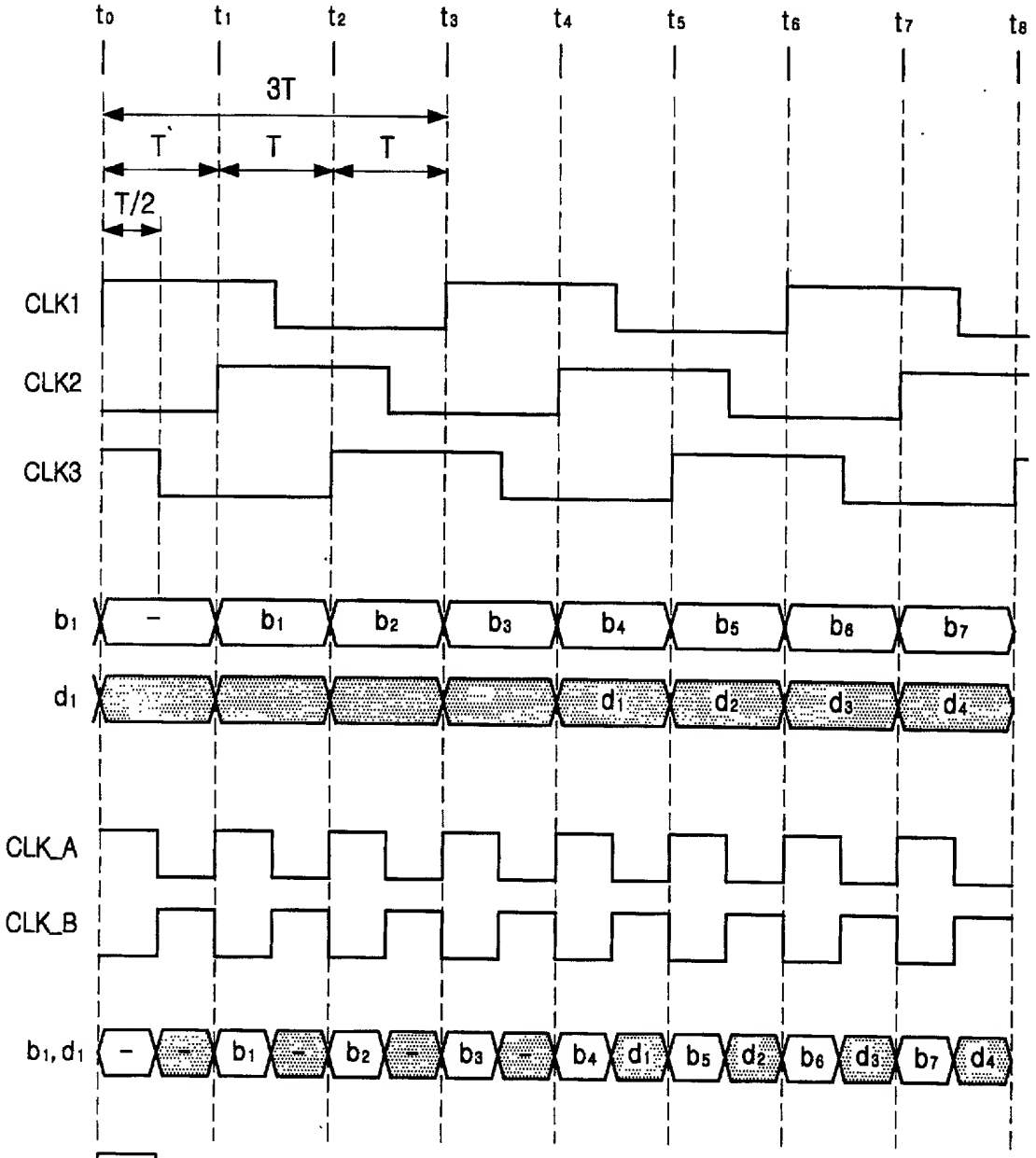

2-port Read Only Memory S-Box
720
S-Box 8
S-Box 1
Path 1
710
48-bit Input
48-bit Input
MULTIPLEXER
6-bit
Address
64 x 4
ROM/PLA
Path 2
4-bit
Data
740
CLK_A
CLK_B
CONTROLLER
DEMULTIPLEXER
730
Path 1
Path 2
32-bit Output
32-bit Output

FIG. 8



–	b1	b2	b3	b4	b5	b6	b7
–	$a_0 \oplus f(b_0, K_1)$	$b_0 \oplus f(b_1, K_2)$	$b_1 \oplus f(b_2, K_3)$	$b_2 \oplus f(b_3, K_4)$	$b_3 \oplus f(b_4, K_5)$	$b_4 \oplus f(b_5, K_6)$	$b_5 \oplus f(b_6, K_7)$

–	–	–	–	d1	d2	d3	d4
–	–	–	–	$c_0 \oplus f(d_0, K_1)$	$d_0 \oplus f(d_1, K_2)$	$d_1 \oplus f(d_2, K_3)$	$d_2 \oplus f(d_3, K_4)$